(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 020 813 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.07.2000 Bulletin 2000/29

(51) Int Cl.7: G06K 19/07, G07F 9/02

(21) Application number: 99309750.0

(22) Date of filing: 06.12.1999

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 11.01.1999 US 228231

(71) Applicant: International Business Machines Corporation
Armonk, NY 10504 (US)

(72) Inventors:
- Chainer, Timothy J., Intellectual Property Law Winchester, Hampshire SO21 2JN (GB)
- Greengard, Claude A., Intellectual Property Law Winchester, Hampshire SO21 2JN (GB)
- Pulleyblank, William R., Intellectual Property Law Winchester, Hampshire SO21 2JN (GB)
- Tresser, Charles P., Intellectual Property Law Winchester, Hampshire SO21 2JN (GB)
- Wu, Chai W., Intellectual Property Law Winchester, Hampshire SO21 2JN (GB)

(74) Representative: Moss, Robert Douglas
IBM United Kingdom Limited
Intellectual Property Department
Hursley Park
Winchester Hampshire SO21 2JN (GB)

(54) Method and apparatus for securely determining aspects of the history of a good

(57) The present invention provides methods and apparatus to detect and reliably record the physical history of a product including effects due to one or more of the following: 1) product use 2) handling 3) tampering and 4) environment of the product (as changes in the environment, such as excessive temperatures, humidity, or shocks, can result in degradation to a product). The apparatus includes a "smart card", or, more generally, "smart token", in combination with one or more sensors which record the external influences on the product and/or the environment and records those changes in an encrypted form. This information can then be verified by any individual who is equipped with a (possibly public) decryption key, but capability to modify this information, depending on the application, is restricted to those with access to the encrypting key. Furthermore, the apparatus contains authentication information which can be reliably verified, in particular to confirm that the apparatus is attached to the product it supposed to be attached to.

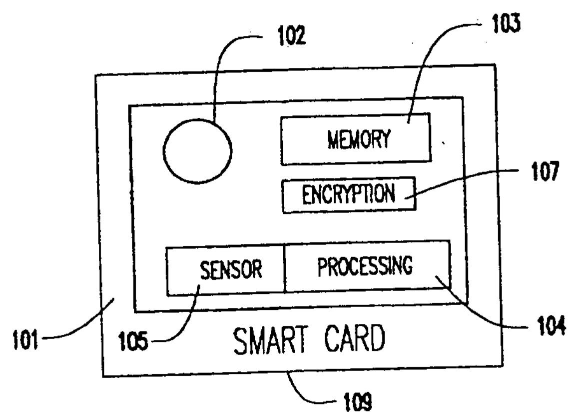

FIG.1B

Description

[0001] The present invention generally relates to security of consumer goods and, more particularly, to the use of smart tags in maintaining product security.

[0002] There is a need for certain products to be equipped with some apparatus which can provide information about the current state of the product as a result of events the product was subjected to prior to becoming in the possession of a potential consumer. Examples include the state of medical or food products prior to their being used by a consumer.

[0003] Also, consumers sometimes have the right and/or the need to know whether a product is brand new or not. This is especially true of expensive items. There is also a need for a product to be equipped by some apparatus which can record some aspects of the product history, for example in the case of automobiles where today odometers indicate, not very securely, one aspect of the history of the automobile.

[0004] Another context for the invention is the fact that, in some cases, the containers of some products are reused by the manufacturer, and the consumer would like to know if the product in the container is new or not, and if the container has been reused by a third, unauthorized, party. There is also a need for a method to detect whether the product has deteriorated, either because of defects, or because its expiration date has passed, or because of unwanted change in the environment, for instance in the form of excessive cold, heat or humidity. These scenarios require an apparatus which can detect the physical forces a product was subjected to as a result of use, handling, tampering or environmental factors. For either human intervention or environmental factors, it may be important in some circumstances that the recorded history of such events be very difficult to modify or counterfeit.

[0005] The prior art contains many methods involving seals and enclosures which allow one to detect when a package has been tampered with. Such prior art go way back in history, and a multitude of improvements, with very general or very specific uses, have been proposed which benefit from the general progress of technology. For example, U.S. Patent No. 5,159,629 to Glen P. Double and Steve H. Weingart describes an intrusion barrier for protecting an electronic assembly from tampering. The prior art also contains methods of recording chronological information such as a data logger which stores information on a product as described in U.S. Patent No. 5,010,560 to Mark A. Janney, Roger Newey, and Irwin J. Robinson.

[0006] However, these methods do not overcome the problem of providing a tamper evident history of a product and/or of its environment. The prior art does not allow the information about the history of a product and/ or of its environment to be securely recorded and kept.

[0007] According to a first aspect, the invention provides a method of recording and storing information in an integrated smart tag about at least one of physical, chemical and environmental effects on an object, over time, comprising the steps of: sensing data regarding a state of said object or an environment of said object, with at least one of a plurality of sensors; and sending a signal from said sensor to a storage device embedded within the smart tag.

[0008] According to a second aspect, the invention provides a smart tag system comprising: a storage device; a sensor for sensing data regarding a state of an object or an environment of an object; and means for sending the sensed data to said storage device.

[0009] In the following, terms such as "impossible to change" or "tamper-proof" should be understood to describe situations in which sufficient resistance to tampering is provided to make successful attacks rare due to cost/benefit issues, since codes, etc., can theoretically be broken if sufficient resources are brought to bear on the attack.

[0010] The invention uses a smart card (also known as smart tag), as described in U.S. Patent Nos. 3,971,916, 4,007,355, 4,092,524, and 4,102,493 to Roland Moreno, or, more generally, a smart token, in combination with sensors attached to the product and/or to the smart card: upon tampering, or as a response to other circumstances, the sensors generate signals which are preferably encrypted and recorded in the memory or storage device of the smart card attached to the product.

[0011] Recall that, for example, by using a zero-knowledge protocol, a smart card can be authenticated but cannot be duplicated. This technology has been disclosed for instance in U.S. Patent 5,140,634 to Guillou, et al. This is the property which characterizes a smart card. Accordingly, in the rest of the present disclosure, any electronic component with these properties and which has some memories and/or some processing capabilities, will be called "a smart token" or "a smart card", even if it does not actually take any form resembling a card. A general reference to smart card technology and applications can be found in Smart Cards: A Guide to Building and Managing Smart Card Applications, by Henry Dreifus and J. Thomas Monk, John Wiley & Sons, 1998.

[0012] When the product or its packaging is tampered with, some attribute of the product or its environment changes. This change is what is detected by (at least some of) the sensors attached to a smart card, and the smart card will record this change irreversibly by erasing or writing some information within the smart card memory. The smart card also can be made duplication resistant by using a zero-knowledge protocol so that only the manufacturer of the original product, and/or possibly a trusted third party, for example, can produce or buy such smart cards. The smart card also can record the history of these changes in its internal memory.

[0013] The foregoing and other objects, aspects and advantages will be better understood from the following

detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure 1A is an isometric diagram showing a smart tag attached to a product;

Figure 1B is a plan view showing detail of the smart tag shown in Figure 1; and

Figure 2 is a schematic diagram showing the path from sensors to production of an electrical signal.

[0014] Referring now to the drawings, and more particularly to Figure 1A, there is shown a smart card 101 attached to a product 106. As shown in Figure 1B, the smart card is powered by a small power source such as a battery 102. In addition to the normal components in a smart card, such as memory or storage device 103 and processing unit 104, and encryption module 107, the smart card is also connected to a sensor 105 (or some number of sensors) which can detect changes in the product and/or the environment due to tampering.

[0015] The encryption module can use any of the well-known (public or private) encryption algorithms such as Rivest, Shamir and Adleman (RSA) or Data Encryption Standard (DES), as described for example in Handbook of Applied Cryptography, by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press, 1997. A discussion on cryptographic issues related to smart cards can be found in the aforementioned book by Dreifus and Monk. The encryption algorithms can be implemented as software modules on the main processor of the smart card, or they can be executed in specialized hardware. An example of such specialized hardware currently used as a cryptographic accelerator to a personal computer is the LunaVPN cryptographic accelerator manufactured by Chrysalis-ITS, Ontario, Canada.

[0016] The entire smart card can be protected by a tamper proof package 109, such as the one described in U.S. Patent No. 5,159,629. The smart card should be tamper evident in the sense that any attempt in determining and/or changing the data in the smart card would result in erasure of this data and/or destruction of some element of the smart card. To prevent tampering with the smart card itself, the packaging can include a trip wire or magnetic circuit forming a closed connection with the sensor and any tampering with the product involves opening the packaging in such a way as to break this connection and trigger an (irreversible) change within the smart card. In certain circumstances the tamper proof feature and encryption may not be necessary.

[0017] Other mechanisms can also be used to the same ends of preventing modifications and/or duplication of the smart card or its data content, examples being obtained as easy modification of the invention in U.S. Patent No. 5,159,629.

[0018] The sensor can also be an on-chip pressure sensor or a pressure sensor such as the NPP, NPC or NPH series pressure sensor manufactured by Lucas NovaSensor of Fremont, California, with the product packaged under low pressure. Tampering with the product necessitates opening the packaging and allowing outside air to reach this sensor. This change in pressure is recorded by the smart card. For improved protection, the package can also contain a pump to randomly vary the pressure inside the package. In this case the pressure sensor measures the pressure, Psensor, inside the package and compares the sensor reading to the processor command, Pcomputer, to the pump. A difference signal can be computed as

$$\text{Pdifference} = \text{Pcomputer} - \text{Psensor}$$

If the Pdifference is greater than a threshold Pthresh, then the package is considered to be tampered with.

[0019] In yet another implementation, the smart card has a light sensor such as the photodetector MTD3010PM made by Marktech Optoelectronics, Latham, New York. The smart card is then packaged so as not to be exposed to light. When the product is tampered with, light will reach this sensor and the smart card will record this change. One may use an optoelectronic sensor which can detect electromagnetic radiation beyond the visual spectrum such as infrared or ultraviolet radiation. Whichever part of the spectrum is used, supplementary sources of radiation can be used, with random levels, as described previously in the case of the pressure sensor, to enhance the security.

[0020] Similarly, a temperature sensor such as the TMP03 series sensors manufactured by Analog Devices, Norwood, Massachusetts, can be used to detect changes in temperature, in applications where the temperature at which a product is shipped has to be maintained in a certain range.

[0021] In applications such as in motor vehicles where the detection of shock is needed, an accelerometer such as the Analog Devices ADXL05 or Lucas NovaSensor NAC series accelerometer can be used as the sensor (or as one of the sensors).

[0022] In one application of a smart tag vehicle sensor, the smart card records the output of the ADXL05, generates a time stamp and encrypts and stores the result into the memory 103 of the smart tag. In addition, other sensors, such as the TMP03 temperature sensor may also be logged and stored. The vehicle speedometer readings and odometer readings may be time stamped, encrypted also stored in the memory 103. The location of the vehicle is often important in indentifying the types of weather conditions the vehicle has been subjected to, and adding a GPS system whose output is securely recorded in memory may also be added. The combination of the time history of the shock, temperature, speed history, mileage history and geographic location can be used to create a secure vehicle history which can be made available to evaluate the condition

of the vehicle.

[0023] An example of such a history is summarized below:

Vehicle History =
mileage
50,000 miles
max shock
10 g
max temperature
90 F
minimum temperature
50 F
max speed
85 mph
vehicle location
Florida 90% of miles
other 10% of miles

[0024] Depending on the product, the sensor (or the combination of sensors) detects mechanical, electromagnetic and thermal properties, and more generally a physical and/or chemical property or a combination thereof. References for sensors detecting chemical properties are found in An Introduction to Electronic Nose Technology, by J. Gardner, Neotronics Scientific, Warwick, 1996. Once a change is detected beyond some fixed threshold (or when the data captured by the sensors differs enough from a computed random sequence) at 105, it will be irreversibly recorded within the smart card 101. Time stamping of the event provides a recorded history for the device; secure time stamping can be achieved for instance by attaching a clock or timing unit to the smart card inside the tamper proof package 109.

[0025] As shown in Figure 2, for instance, using such physical properties as piezoelectricity, the sensor 105 such as a Murata PDGS-00LA-TC accelerometer produces a voltage 113 in response to an external force input which results in an acceleration of the sensor. When the electronic signal 113 exceeds some predetermined threshold 110 a comparator 111 is triggered to produce a logic level output to power up the smart card. As a consequence, once a shock is detected greater than a predetermined threshold, it will be irreversibly recorded as a change within the smart card 101. This same concept could be adapted to accommodate random input as an additional means to protect against entering a package containing a product.

[0026] The recorded data is encrypted and provides a history of physical events of the product. Anybody in possession of a (possibly public) key can retrieve the data which, once processed by proper algorithms, allows determination of the product state, and allows recognition that the smart card is attached to the product to which it is supposed to be attached. Such analysis can include, but is not limited to, the temperature to which the product was subjected, shocks the product experienced, the first time the product was powered on, etc.

[0027] In some cases, if needed, the smart card will also keep a record of the history of changes by also recording the time. In all cases, the change in the product or its environment causes the state of the smart card to be changed irreversibly. This can be effected by the smart card erasing or writing some information in its internal memory.

[0028] Any person wishing to determine whether the product is new or not first authenticates the smart card using a zero knowledge protocol. He or she then queries the smart card for the information on whether the product has been opened or been tampered with. If both the authentication is successful and the smart card did not record any change in state, then it can be concluded that the product has not been tampered with.

[0029] The smart card can be contactless (by which we mean that no physical contact with the card is needed when performing the authentication or querying) and is embedded into the product or its container: In this case, the authentication and query is made via some remote means. Such technology is currently available. For instance, in RFIDS as disclosed in U.S. Patent No. 5,682,143 to Michael J. Brady, Thomas Cofino, Harley K. Heinrich, Glen W. Johnson, Paul A. Moskovitz, and George F. Walken. For early references, see, for example, U.S. Patent No. 4,063,229 to John Welsh and Richard N. Vaughan, U.S. Patent No. 4,242,663 to Leo Slobodin, and U.S. Patent No. 4,646,090 to Daniel D. Mawhinney.

[0030] For certain products, the output of the sensor 105 is sent to processor 104 which executes a mathematical algorithm to determine a function of the history of the object and/or its environment. For example, milk containers temperature and time history can be used to determine the probability that the milk is sour according to a model, such as shown below:

where T is the temperature of the milk container, t is time, and f is a function which can be determined experimentally. The process can result in a message which may or may not be encrypted. For instance, the message may be a visible indicator to the consumer.

[0031] Some products (such as wine, food, chemical compounds, or pharmacological products) can deteriorate with no known cause, in which case one cannot use only the control of the environment, but some sensor has to detect intrinsic chemical and/or physical properties of the product. The inventive device could be used to record temperature, humidity, pressure, light, vibration, shock, electromagnetic field, chemical composition, and the opening of the packaging which contain the products.

[0032] If the passing of the expiration date is to be detected, the smart card is equipped with a clock or timer which would record the expiration of the product when it occurs.

[0033] In another embodiment, the inventive device may be used for detecting and recording changes in consumer electronic products. In addition, to the chang-

es described previously, hours of in-use time (power-on hours) for product may be recorded.

[0034] The smart card may be created in an inactive state. After the smart card is attached to the product, the smart card is activated by sending a command to the smart card. This can be done remotely in the case of contactless smart cards. Once activated, the smart card will start monitoring the product and/or its environment. For added security, once activated the smart card cannot be deactivated unless it is destroyed. Alternatively, deactivation would cause an irreversible change in the smart card indicating that the smart card was deactivated after activation.

[0035] In yet another preferred embodiment, the smart card could be powered externally, for example by an RF (radio-frequency) energy source. The smart card has micromachined features on chip which are changed (for example, pieces could be broken off) when the product is tampered with. When the user needs to determine whether the product is tampered with, an external power source is applied to power on the smart card. The authentication phase is as before. Next, the micromachined features are sensed either by the smart card or by the user to determined whether tampering has occurred.

[0036] The present invention provides methods and apparatus to detect and reliably record the physical history of a product including effects due to one or more of the following: 1) product use 2) handling 3) tampering and 4) environment of the product (as changes in the environment, such as excessive temperatures, humidity, or shocks, can result in degradation to a product). The apparatus includes a "smart card", or, more generally, "smart token", in combination with one or more sensors which record the external influences on the product and/or the environment and records those changes in an encrypted form. This information can then be verified by any individual who is equipped with a (possibly public) decryption key, but capability to modify this information, depending on the application, is restricted to those with access to the encrypting key. Furthermore, the apparatus contains authentication information which can be reliably verified, in particular to confirm that the apparatus is attached to the product it supposed to be attached to.

Claims

1. A method of recording and storing information in an integrated smart tag about at least one of physical, chemical and environmental effects on an object, over time, comprising the steps of:

   sensing data regarding a state of said object or an environment of said object, with at least one of a plurality of sensors; and

   sending a signal from said sensor to a storage device embedded within the smart tag.

2. A method as in claim 1 further comprising the step of:

   securely recording said signal using encryption of said signal in said storage device for later retrieval.

3. A method as in claim 1 or 2 further comprising the step of recording a time in said storage device for each said signal sent to said storage device.

4. A method as in claim 1, 2 or 3 wherein said sensors detect changes in one or more states of the of the object selected from the group comprising temperature, humidity, pressure, light, vibration, shock, electromagnetic field, and chemical composition.

5. According to any preceding claim, a method further comprising the steps of:

   processing said sensed data to compute at least one of a plurality of functions of said data; and

   storing a combination of said data and values of said functions in a storage device.

6. A smart tag system comprising:

   a storage device;

   a sensor for sensing data regarding a state of an object or an environment of an object; and

   means for sending the sensed data to said storage device.

7. The system of claim 6 further comprising an encryption means for encrypting said sensed data which is being stored in the storage device.

8. The system of claim 6 or 7 further comprising a processing unit which acts upon said sensed data from said sensor to determine if said sensed data meets a threshold for recording in said storage device.

9. The system of claim 6, 7 or 8 further comprising

   a processor for computing one of a plurality of functions of said sensed data, and

   means for storing said sensed data and values of said functions of said sensed data in the storage device.

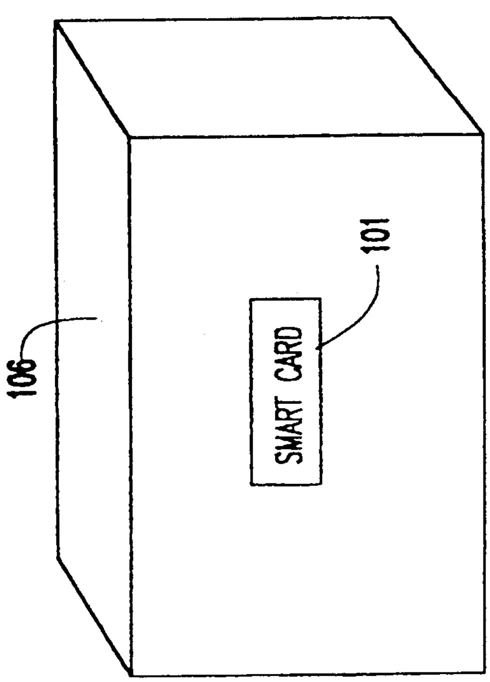
106
SMART CARD
101

FIG.1A

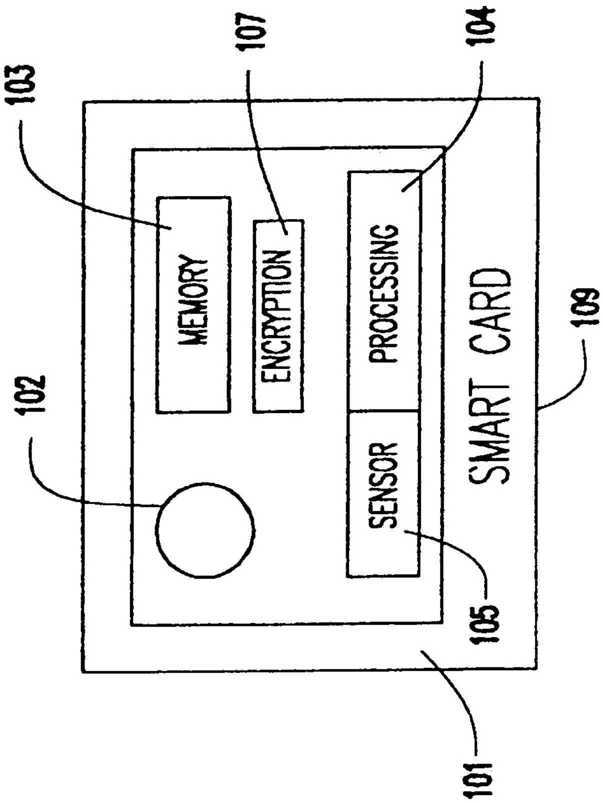
103
107
104
102
MEMORY
ENCRYPTION
PROCESSING
SENSOR
SMART CARD
109
105
101

FIG.1B

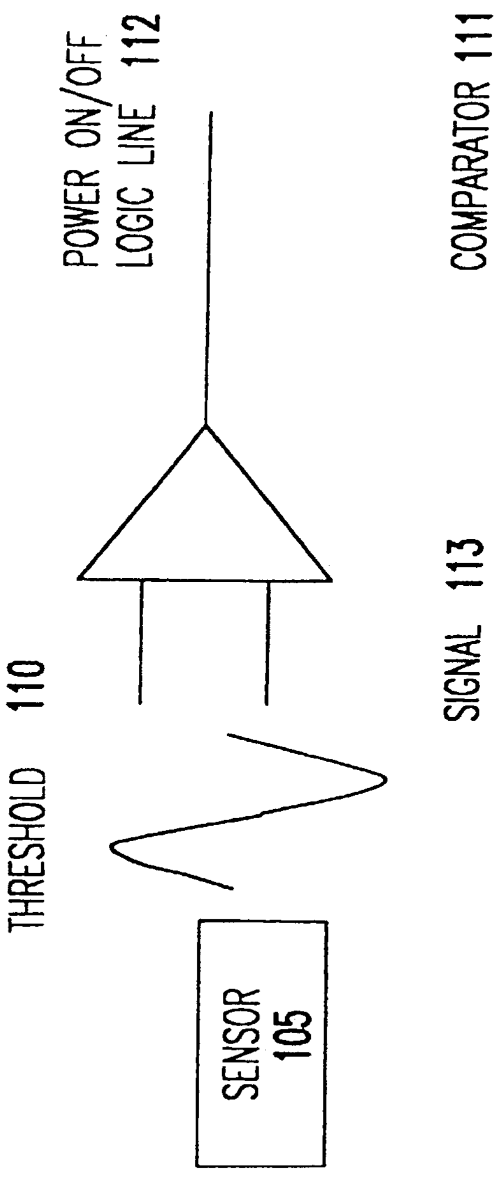
POWER ON/OFF
LOGIC LINE 112
COMPARATOR 111
SIGNAL 113
THRESHOLD 110
SENSOR
105

FIG.2